MOMs* in the NAS
the Challenge of the New Millennium

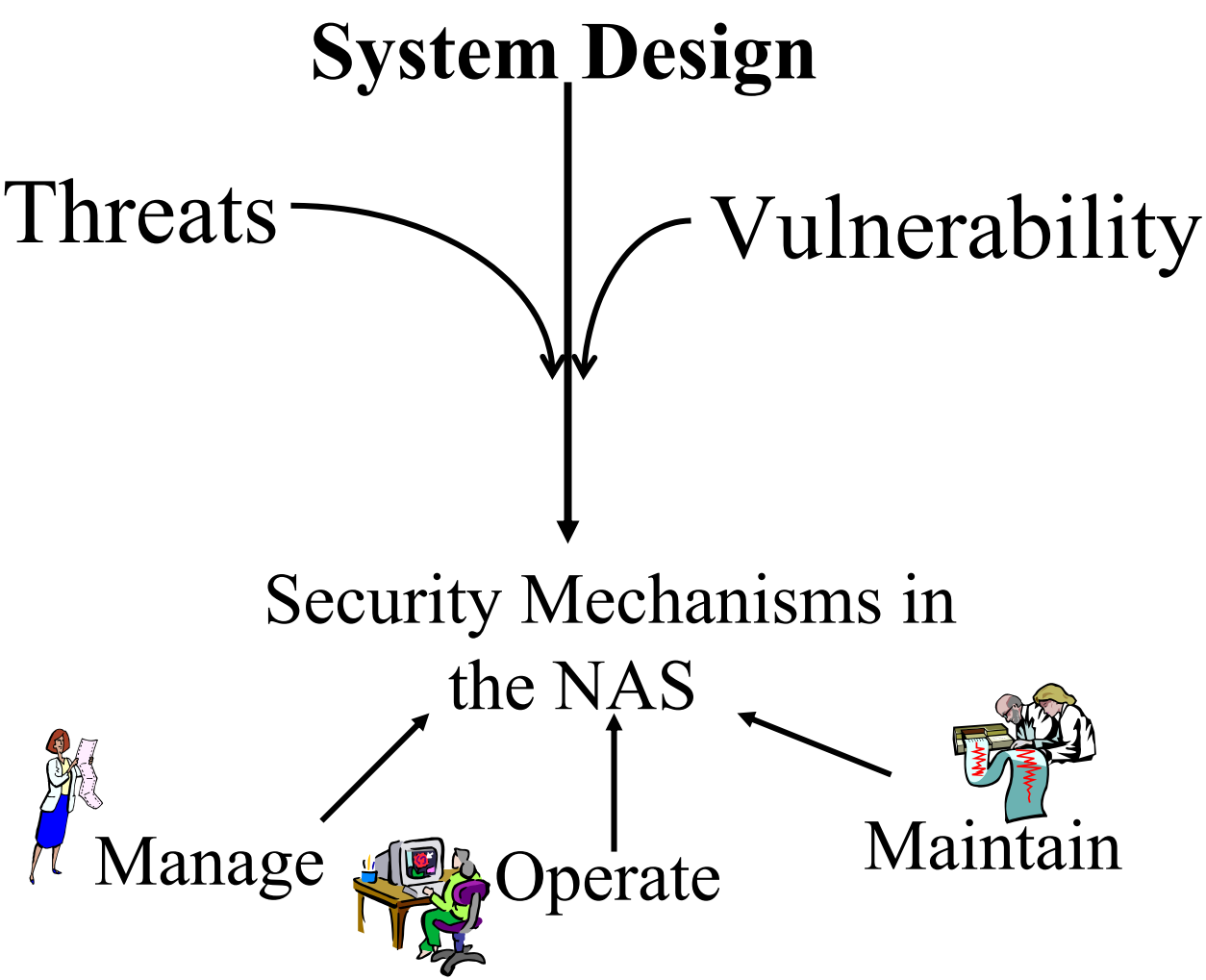
By Marie Stella, CISSP

May 22, 2003

marie.stella@faa.gov

*Management, Operation, and Maintenance of the Information Assurance of the NAS under current national preparedness and economic conditions

Agenda



Changing face of the NAS

National Air Space (NAS)

New Paradigm

Pre 9/11

"Catastrophic events - Safety and loss of life"

Post 9/11

"Economic impact on Nation of loss of confidence in the NAS"

New NAS – not only safety of flight but must address national preparedness and emergency that consists of sonar and sub-sonar traffic

Evolution of NAS Real Estate

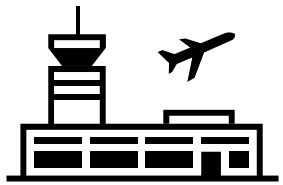
1980s

Design Specifications

Proprietary and arcane OS/SW legacy systems

Limited External communications

Security by Obscurity Low emphasis on system security



1990s

Functional Specifications instead of design specs

COTS/GOTS with known vulnerabilities

Open Communications with trusted/untrusted partners

System Specific security assessments

2000

COTS/GOTS in NAS with no insight, access or documentation rights to code

Multiple security solutions increased implementation, integration, and maintenance problems

Federated NAS with different security requirements

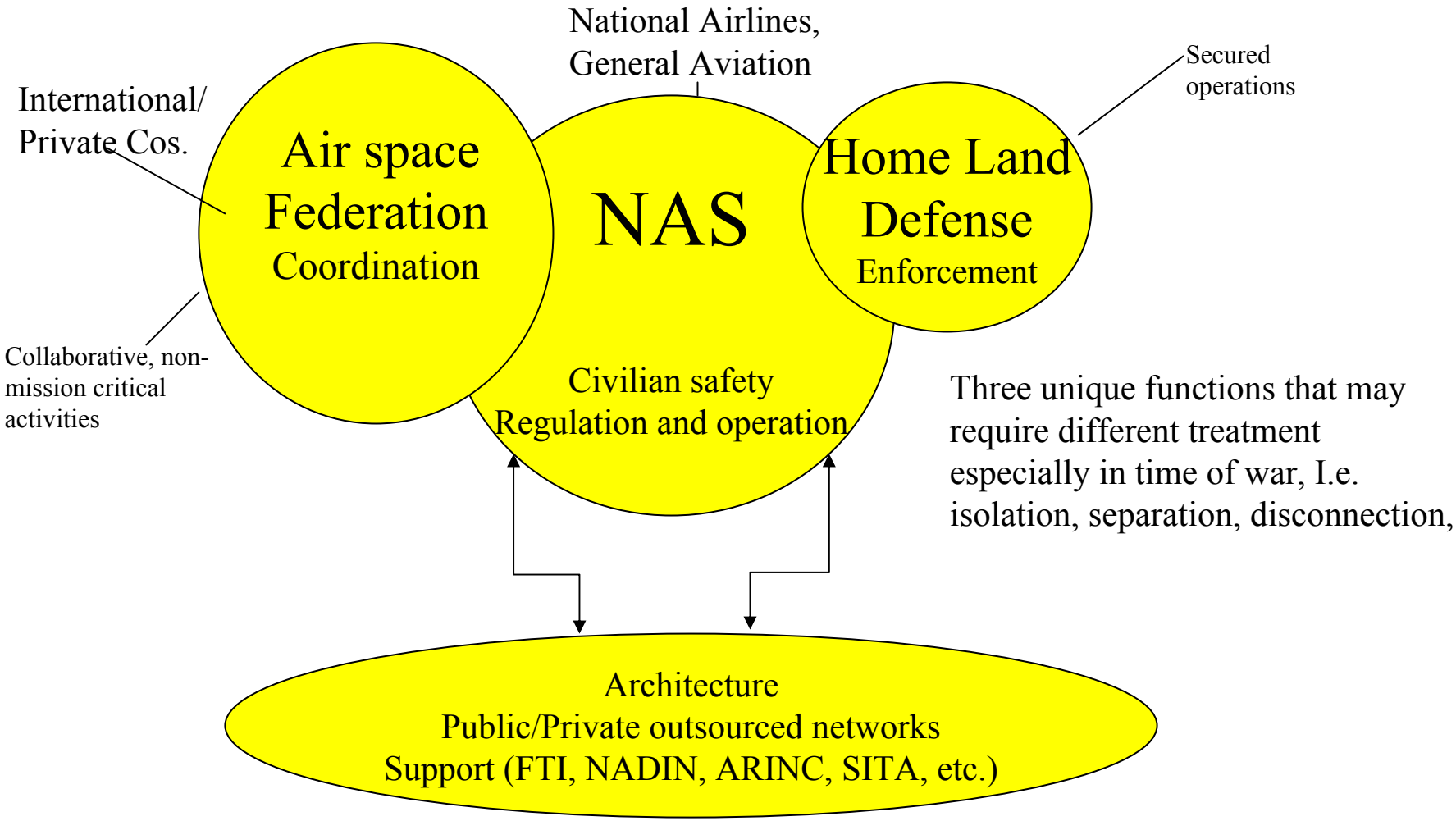
…….

. . . . . .

FEDERATED NAS SECURITY CONCEPT AND LIFE CYCLE IMPLEMENTATION PLAN

(MOM)

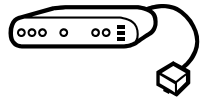
NAS Relations -The New Federation



Three unique functions that may require different treatment especially in time of war, I.e. isolation, separation, disconnection,

NAS INFRASTRUCTURE

Ground Systems:



COTS (?), GOTS, Legacy, which will not be completely replaced for 20 years (Routine and critical systems)

Some COTS system components do not meet NAS RMA or avionics 178B requirements

System by System security approach mandated by OMB, NIST, and FAA proliferates non-interoperable security products such as firewalls, access control and encryption, IDS, virus checkers, etc.

No Government-wide or FAA policies for standards, protocols, security mechanisms, software validation for the air-ground or ground-ground environment especially ones that are compatible with DoD

No strategic plan or vision for a secure NAS that includes life cycle MOMs not an easy problem!

Range of security needs – A and I

NAS INFRASTRUCTURE

Federated NAS

International Data Communication Community

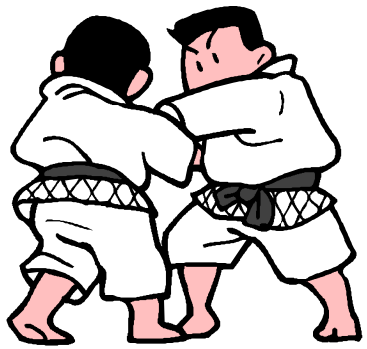
- •ARINC, SITA shared networks
- •Hostile and friendly nations
- •Ground systems

Partners

- •Airlines
- •Weather Services

Common Carriers/Communication Systems

- •FTI
- •Legacy networks
- •ARINC

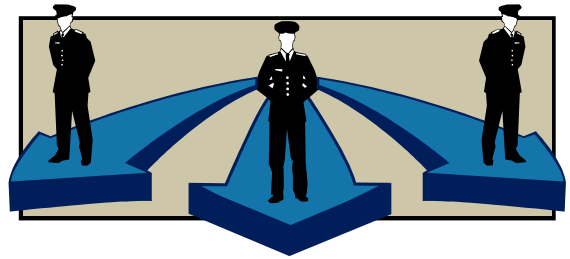


Range of security needs – A and I

Routine to Critical systems

Concept to jointly MOM – especially as it relates to the critical
NAS is very hard – different agendas

NAS INFRASTRUCTURE



Secure NAS

- Homeland Security and DoD Partners
- Surveillance, Navigation, and Communication Systems

Range of security needs – A and I

and C

They are all critical systems and we need to jointly MOM

NAS Ground Infrastructure

Remote Access and Control

NAS requirement for Remote management, however, little progress has been made in this area

- No standards – Equipment supports varied OS with limited and sometimes non-secured capability
- NAS-wide Security Maintenance Policies are not in existence or inadequate
- Do not have a SOC or CSIRC for the NAS
- Security System Administration training is not adequately provided
- No detection,isolation, and restoral policy and procedures

COTS systems with no insight into code

- Zombies, Time bombs, Trojans, etc.
- Spy ware (UCITA) – legal and illegal
- No standard for virus checkers and patches and no standard for detecting, fixing, testing, certifying and downloading

Business Best Practices that we would expect from health care providers and financial institutions

Need to develop Threat Scenarios

Realistic possibility Terrorist Attacks on the critical infrastructure

- Inexpensive
- Easily understood and available attack technologies
- Big bang for the buck

Feasible and well know ways to attack the air-to-ground links

Feasible and well know ways to attack the ground-to-ground link

What are effects of:

- Cyber (air-to-ground, system) compromise that causes accident – Commercial/commercial, commercial/GA commercial/military
- Cyber compromise that has intermittent effects on the NAS and causes Chaos

Influence National and NAS Policy

Government policies encourage poor security practices

- Homeland Defense allows development of security software overseas
- COTS systems software and hardware used ubiquitously developed in (hostile cyber warfare) foreign countries
- Off-shore development of IT software
- Exporting of crypto algorithms
- Access of service provider records – (forensics analysis and prosecution) and outsourcing of services

Short term impact –possible undetected compromised systems and lack of knowledge to isolate and restore

Long term – Brain drain

Immediate Security Needs

A CONOPS for managing operating and maintaining the NAS during normal operations and in times of compromise or national emergency:

- Detection and coordination strategies for compromises to the NAS
- Disconnection of compromised systems and perhaps NAS/aircraft non-critical communication
- Isolation of the critical NAS/NAS-Homeland Defense components
- Implementation of as-needed basis security mechanisms, I.e., authentication, integrity, audit and possibly confidentiality
- Defined roles and responsibilities of NAS personnel and NAS partners to perform these activities
- Cooperative plan to restore compromised systems

Long-Term Research Suggestions

Assessment of future air-to-ground protocols and technologies for security vulnerabilities and develop mitigation strategies

IDS and firewalls for non-IP NAS protocols that are well know and easy to attack

Performance based (non-intrusive) IP IDS and firewalls

Voice and data authentication methodologies A-G/G-G

Methods to provide confidentiality perhaps on an as-needed basis

Alternative methods of situational awareness in the event of compromise

Automated methods to evaluate source code, software

Common goal of meeting the FAA Mission – collaboration and standards